This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) In a computing device, a method for protecting sensitive files from unauthorized access, comprising:

detecting a connection of the computing device to an electronic device;

accessing an authorized connection list;

determining whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

accessing sensitive file information which identifies at least one sensitive file stored on the computing device; and

preventing access to the at least one sensitive file identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list.

2. (Original) The method of claim 1, wherein if the connection is not identified in the authorized connection list the method further comprises:

detecting termination of the connection; and

if the computing device does not have any other unauthorized connections, restoring access to the at least one sensitive file identified by the sensitive file information.

3. (Original) The method of claim 1, wherein the connection occurs via a computer network.

4. (Original) The method of claim 3, wherein the network is a wireless network, and wherein the computing device is a mobile computing device.

5. (Original) The method of claim 1, wherein the connection is a direct connection.

6. (Currently Amended) The method of claim 1, wherein ~~preventing access to the at least one sensitive file~~ the access prevention task comprises locking the at least one sensitive file.

7. (Currently Amended) The method of claim 1, wherein ~~preventing access to the at least one sensitive file~~ the access prevention task comprises encrypting the at least one sensitive file.

8. (Currently Amended) The method of claim 1, wherein the computing device comprises a storage device, and wherein ~~preventing access to the at least one sensitive file~~ the access prevention task comprises moving the at least one sensitive file to a host-protected area of the storage device.

9. (Original) The method of claim 1, wherein the sensitive file information is a reference to a directory in which the at least one sensitive file is stored.

10. (Original) The method of claim 1, wherein the sensitive file information is a list of the at least one sensitive file.

11. (Original) The method of claim 1, wherein the authorized connection list comprises a list of at least one authorized network.

12. (Original) The method of claim 1, wherein the authorized connection list comprises a list of at least one authorized connection type.

13. (Currently Amended) In an administrative system which distributes software to a plurality of computing devices on an enterprise network, a method comprising:

providing a security agent, wherein after installation on a computing device the security agent is configured to implement a method comprising:

detecting a connection of the computing device to an electronic device;

accessing an authorized connection list;

determining whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

accessing sensitive file information which identifies at least one sensitive file stored on the computing device; and

preventing access to the at least one sensitive file identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list; and

transmitting the security agent to the plurality of computing devices via the enterprise network.

14. (Original) The method of claim 13, further comprising:

providing the authorized connection list;

providing the sensitive file information; and

transmitting the authorized connection list and the sensitive file information to the plurality of computing devices via the enterprise network.

15. (Currently Amended) A computing device that is configured for protecting sensitive files from unauthorized access, comprising:

a processor;

memory in electronic communication with the processor; and

instructions stored in the memory, the instructions being executable to implement a method comprising:

detecting a connection of the computing device to an electronic device;

accessing an authorized connection list;

determining whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

accessing sensitive file information which identifies at least one sensitive file stored on the computing device; and

preventing access to the at least one sensitive file identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list.

16. (Original) The computing device of claim 15, wherein if the connection is not identified in the authorized connection list the method further comprises:

detecting termination of the connection; and

if the computing device does not have any other unauthorized connections, restoring access to the at least one sensitive file identified by the sensitive file information.

17. (Currently Amended) The computing device of claim 15, wherein ~~preventing access to the at least one sensitive file~~ the access prevention task comprises at least one of locking the at

least one sensitive file, encrypting the at least one sensitive file, and moving the at least one sensitive file to a host-protected area of a storage device.

18. (Currently Amended) A computer-readable medium for storing program data, wherein the program data comprises executable instructions for implementing a method comprising:

detecting a connection of a computing device to an electronic device;

accessing an authorized connection list;

determining whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list:

accessing sensitive file information which identifies at least one sensitive file stored on the computing device; and

preventing access to the at least one sensitive file identified by the sensitive file information by performing an access prevention task after the connection is not identified in the authorized connection list.

19. (Original) The computer-readable medium of claim 18, wherein if the connection is not identified in the authorized connection list the method further comprises:

detecting termination of the connection; and

if the computing device does not have any other unauthorized connections, restoring access to the at least one sensitive file identified by the sensitive file information.

20. (Currently Amended) The computer-readable medium of claim 18, wherein ~~preventing access to the at least one sensitive file~~ the access prevention task comprises at least one of locking the at least one sensitive file, encrypting the at least one sensitive file, and moving the at least one sensitive file to a host-protected area of a storage device.